Josh Van Edward D. Abanico

Report di Penetration Testing

Esercizio Pratico: Sfruttamento Vulnerabilità vsftpd con Metasploit

19 Gennaio 2026

Sommario

Il documento riporta i dettagli tecnici dell'attività di Penetration Testing condotta contro una macchina virtuale target (Metasploitable). L'obiettivo dell'esercizio è stato identificare, sfruttare e verificare una vulnerabilità critica nel servizio FTP (vsftpd 2.3.4) per ottenere l'accesso remoto con privilegi di root e modificare il file system del target.

Indice

1 Introduzione e Scenario

Come richiesto dalle specifiche dell'esercizio, è stata condotta una sessione di hacking etico utilizzando il framework **Metasploit** su sistema operativo Kali Linux.

1.1 Obiettivi dell'Attività

- Identificazione del servizio vulnerabile sulla macchina target.
- Configurazione dell'exploit specifico per *vsftpd 2.3.4 Backdoor*.
- Esecuzione dell'attacco per ottenere una reverse shell.
- Post-exploitation: Creazione di una directory di prova (`test_metasploit`) per confermare i privilegi acquisiti.

1.2 Ambiente di Test

- **Attacker Machine:** Kali Linux (IP: Dinamico/Locale)
- **Target Machine:** Metasploitable 2
- **Target IP:** 192.168.1.149 (come da specifiche traccia)
- **Servizio Target:** vsftpd 2.3.4 (Porta 21)

2 Metodologia ed Esecuzione

2.1 Fase 1: Avvio del Framework

La sessione è iniziata con l'avvio della console di Metasploit (`msfconsole`) sulla macchina attaccante.

Figura 1: Avvio di Metasploit Framework (msfconsole).

2.2 Fase 2: Ricerca della Vulnerabilità

È stata effettuata una ricerca nel database degli exploit di Metasploit per il servizio `vsftpd`. La ricerca ha restituito il modulo `exploit/unix/ftp/vsftpd_234_backdoor`, noto per permettere l'esecuzione di comandi arbitrari tramite una backdoor introdotta nel codice sorgente di questa specifica versione.

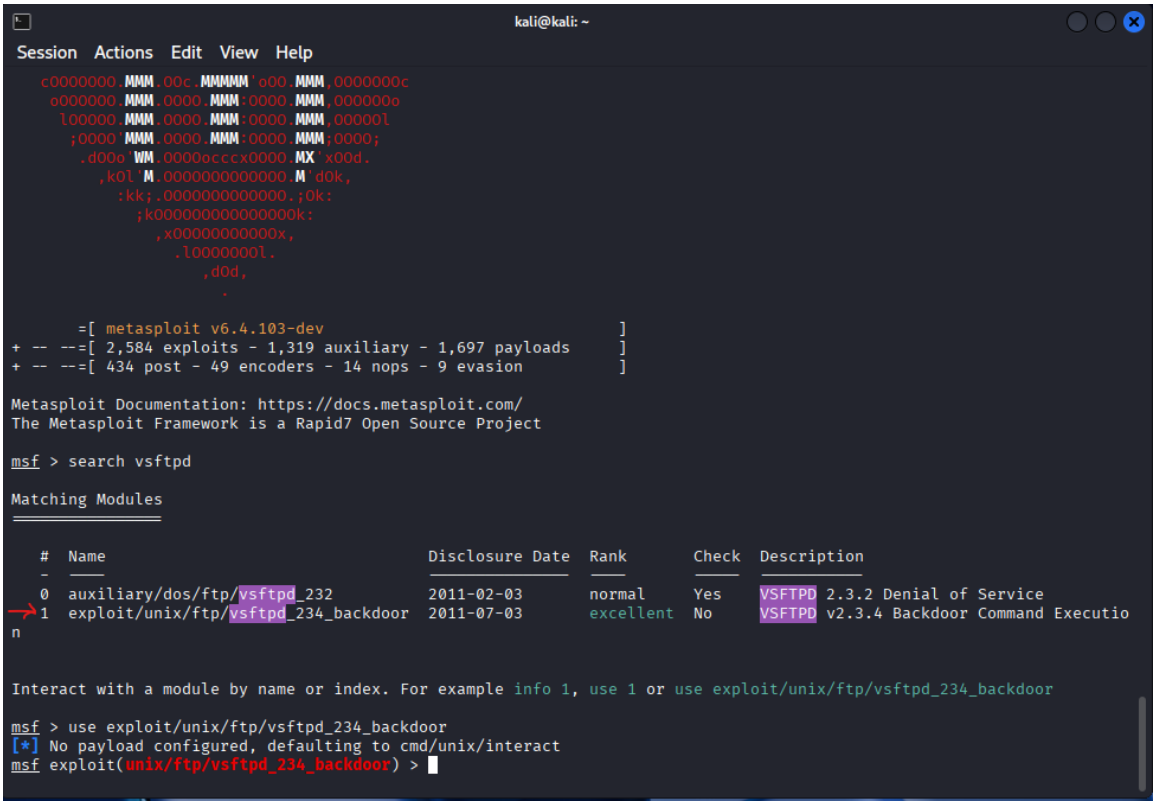

Figura 2: Ricerca del modulo exploit per vsftpd.

2.3 Fase 3: Configurazione dell'Exploit

Una volta selezionato il modulo corretto, sono stati configurati i parametri necessari. In particolare, è stato impostato l'indirizzo IP del target (`RHOSTS`) su **192.168.1.149**, come indicato nella traccia dell'esercizio.

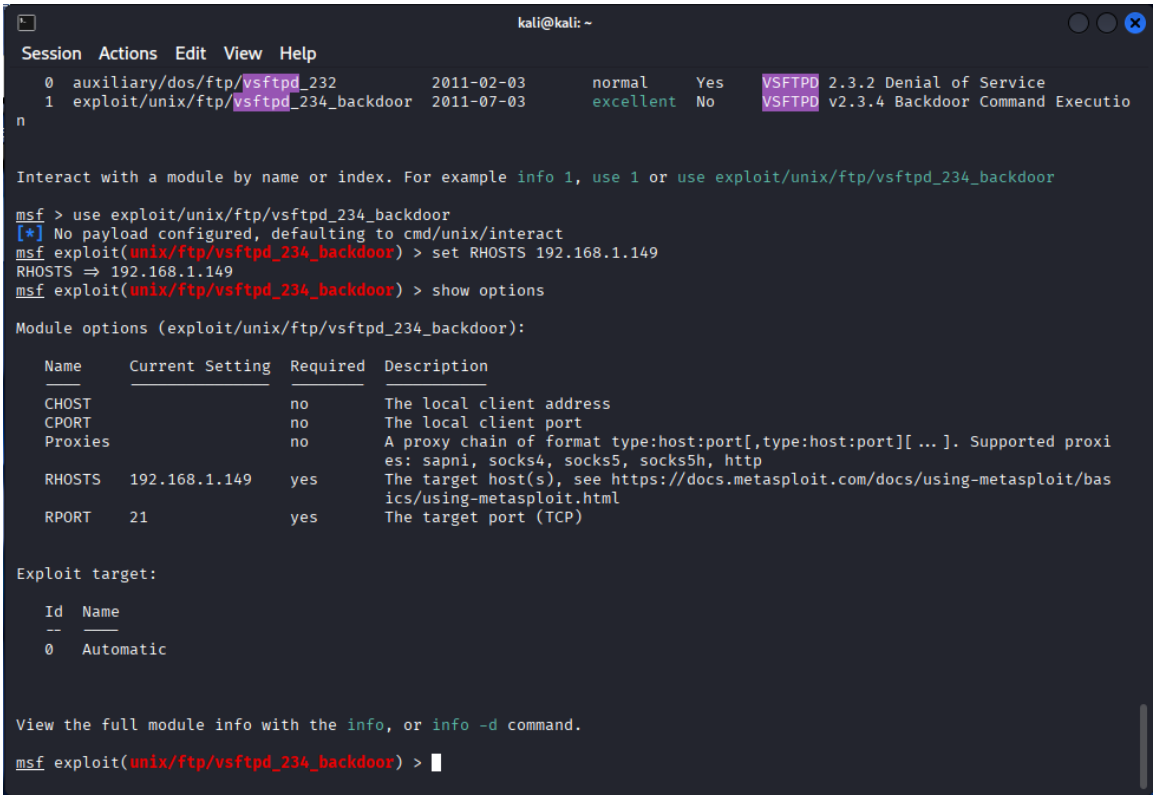

Figura 3: Configurazione del target RHOSTS a 192.168.1.149.

2.4 Fase 4: Exploitation

Lanciando il comando `exploit`, Metasploit ha stabilito con successo una connessione alla porta 21 del target, attivando la backdoor. Il sistema ha aperto una shell di comando (Session 2) con privilegi di root (UID 0), garantendo il controllo completo della macchina vittima.

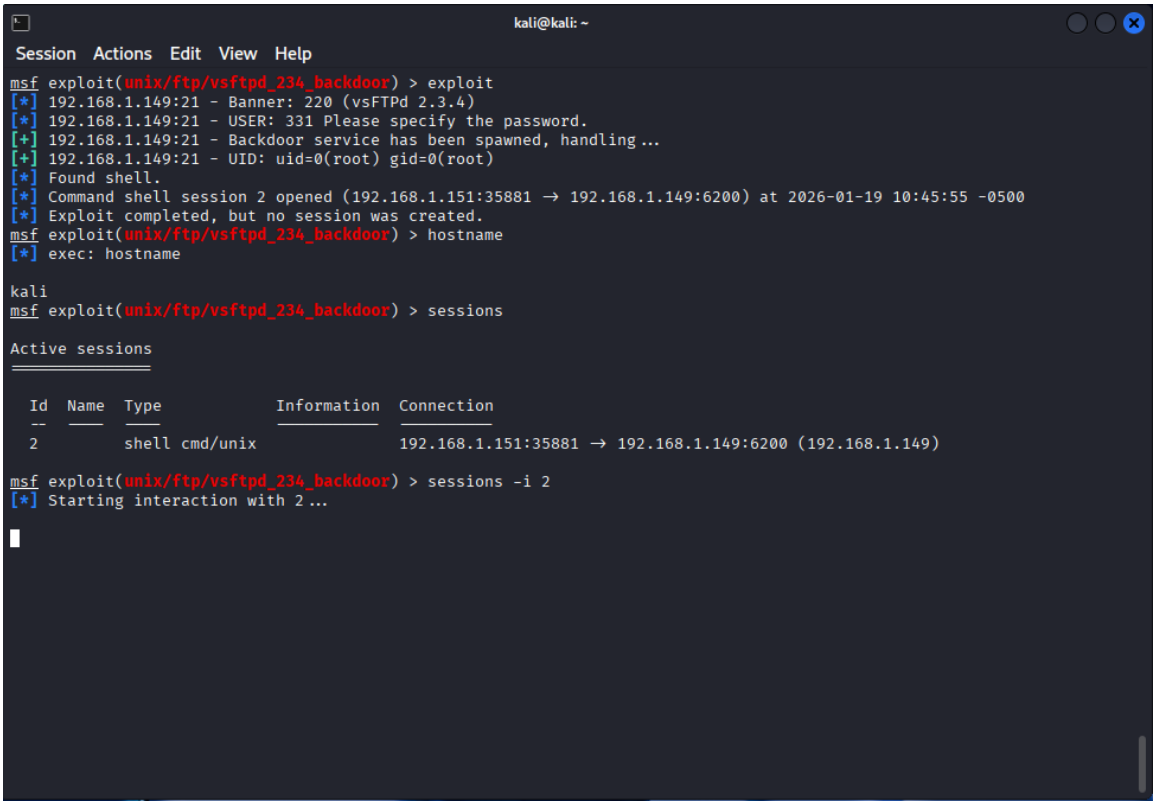

Figura 4: Esecuzione dell'exploit e apertura della shell di root.

3 Post-Exploitation e Verifica

3.1 Esecuzione Comandi su Target

Per confermare l'accesso e completare l'esercizio, sono stati eseguiti i seguenti comandi all'interno della shell compromessa:

1. `pwd` e `ls`: Per verificare la posizione attuale e il contenuto della directory.
2. `mkdir test_metasploit`: Per creare la cartella richiesta dalla traccia dell'esercizio.
3. `ls`: Per confermare l'avvenuta creazione della cartella.

Figura 5: Creazione della directory "test_metasploit" tramite shell remota.

3.2 Verifica Lato Vittima

Come prova finale dell'efficacia dell'attacco, è stata verificata la presenza della directory direttamente sulla macchina Metasploitable. Lo screenshot sottostante mostra il filesystem della vittima modificato dall'attaccante.

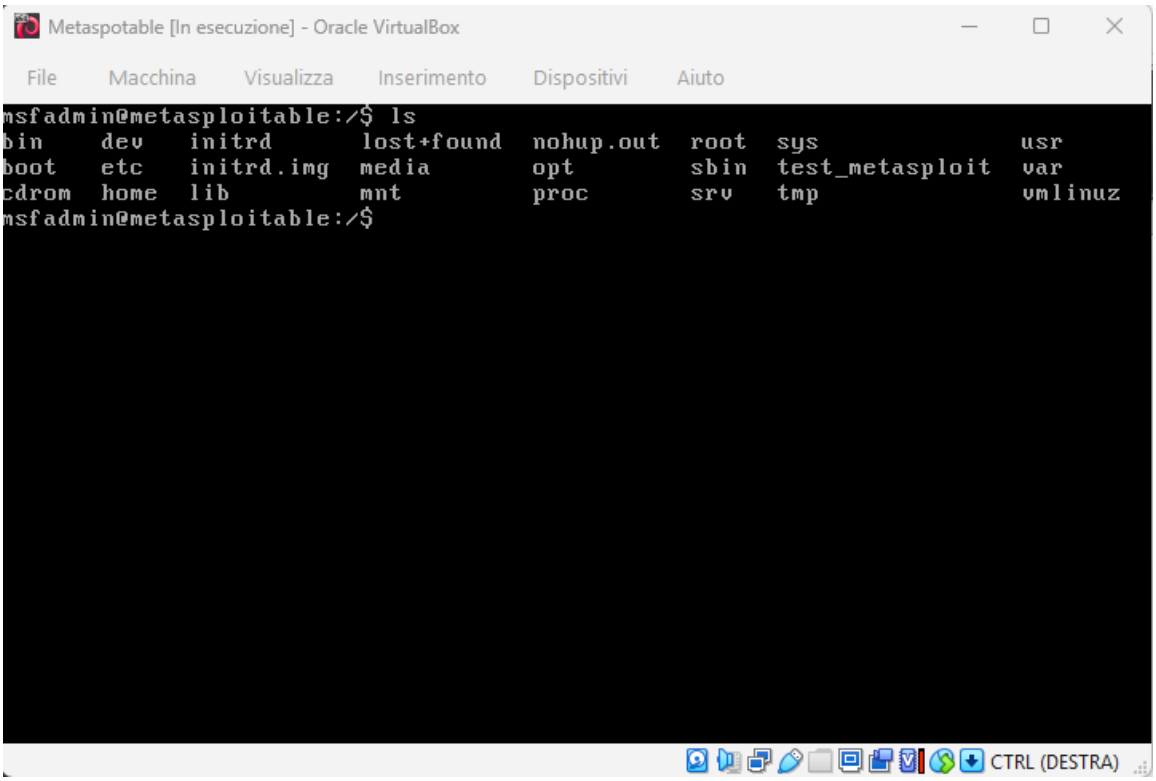

Figura 6: Verifica della cartella creata sulla macchina Metasploitable.

4 Conclusioni

L'esercizio ha dimostrato con successo la vulnerabilità critica presente nella versione 2.3.4 di vsftpd. L'attacco ha permesso l'acquisizione immediata dei privilegi di root senza necessità di autenticazione.

Si raccomanda, in un ambiente di produzione reale, di aggiornare immediatamente il servizio FTP a una versione patchata e di implementare regole firewall per limitare l'accesso alle porte di gestione.